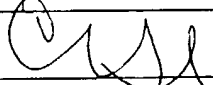


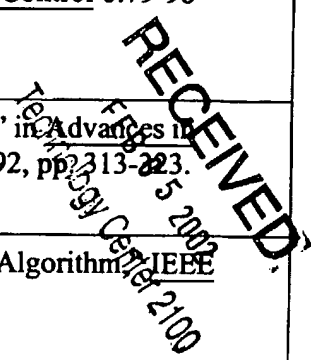
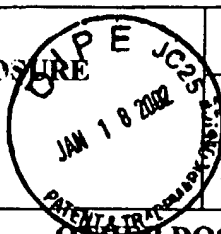
#5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Docket: 245-53434		App: 09/621,020	
		Applicant: Tenca et al.			
		Filed: July 21, 2000		Art Unit:	
OTHER DOCUMENTS					
UN			Menezes, J. et al., <u>Handbook of Applied Cryptography</u> , CRC Press, 1996, pp. 660-603.		
UN			Even, S., "Systolic Modular Multiplication," <u>Advances in Cryptology, Proceedings Crypto 90</u> , Lecture Notes in Computer Science, vol. 537, A. J. Menzes et al., pp. 619-624 (1991).		
UN			Bosselaers, A. et al., "Comparison of three modular reduction functions," <u>Advances in Cryptology, Proceedings Crypto 93</u> , pp 175-186 (1996).		
UN			Koç, Ç. et al., "Carry-Save Adders for Computing the Product AB Modulo N," <u>Electron. Lett.</u> , 26:899-900 (1990).		
UN			Agnew, G. et al., "Arithmetic Operations in $GF(2^m)$," <u>J. of Cryptology</u> , pp. 3-13 (1993).		
UN			Koç, Ç. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," <u>IEEE Micro</u> , 16:26-33 (June 1996).		
UN			Koç, Ç., "Montgomery reduction with even modulus," <u>IEE Proc.-Comput. Digit. Tech.</u> , 141:314-316 (September 1994).		
UN			Paar, C., et al., "Fast Arithmetic Architectures for Public-Key Algorithms over Galois Fields $GF((2^n)^m)$," <u>Eurocrypt '97</u> , May 11, 1997, pp. 363-378.		
UN			Leu, J., et al., "A Scalable Low-Complexity Digit-Serial VLSI Architecture For RSA Cryptosystem," in <u>IEEE Workshop on Signal Processing Systems</u> 1999, pp. 586-595.		
EXAMINER:				DATE 8/4/04	
<p>*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.</p>					

BEST AVAILABLE COPY

#6

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Docket: 245-53434		App: 09/621,020	
		Applicant: Tenca et al.			
		Filed: July 21, 2000		Art Unit:	
OTHER DOCUMENTS					
[Initials]	[Initials]	[Initials]	Bartee, T., et al., "Computation with Finite Fields," <u>Inform. and Control</u> 6:79-98 (1963).		
[Initials]	[Initials]	[Initials]	Walter, C., "Faster Modular Multiplication by Operand Scaling," in <u>Advances in Cryptology Proc. Crypto '91</u> , LNCS 576, J. Feigenbaum, ed., 1992, pp. 313-323.		
[Initials]	[Initials]	[Initials]	Bajard, J. et al., "An RNS Montgomery Modular Multiplication Algorithm," <u>IEEE Trans. Computers</u> 47:766-776 (July 1998).		
[Initials]	[Initials]	[Initials]	Koç, Ç., et al., "Montgomery Multiplication in $GF(2^k)$," <u>Designs, Codes and Cryptography</u> 14:57-69 (April 1998).		
EXAMINER: [Signature]		DATE 8/4/04			
*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.					



BEST AVAILABLE COPY